Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

and, Hardy and Riesz's *The general theory of Dirichlet's series* (Cambridge, 1915), 147–150; Review by A. C. D. Crommelin of Plummer's *An introductory treatise on dynamical astronomy* (Cambridge, 1918), 150–152.

The Tôhoku Mathematical Journal, volume 15, nos. 3–4, April, 1919: "Note on Laguerre transformations," 227–231; "On Steiner's problem of closure" by K. Yanagihara, 232–235; "On curves with monotonous curvature" by T. Hayashi, 236–239; "Note on determinants whose matrix is that of an orthogonant increased or diminished by matrix unity," by T. Muir, 240–245; "On the sign and magnitude of the coefficients in the Fourier series, the sine series and the cosine series" by K. Ogura, 246–260; "Tractories in the irreversible field of force on a surface" by K. Ogura, 261–277; "A theorem on power series" by Y. Okada, 278–279; "A theorem on limits" by Y. Okada, 280–283; "An extension of a theorem of Scheefer's" by Y. Uchida, 284; "Ueber eine Ungleichung für bestimmte Integrale" by M. Jujiwara, 285–288; "Casey's Theorem in Japanese Mathematics" by T. Hayashi, 289–296 (in Japanese); "On Mr. Ône's theorem" by K. Ôishi, 297–299; "Some theorems on limits" by S. Narumi, 300–313; "Einige Sätze den Grenz wert betreffend" by T. Kubota, 314–322; "Ueber summierbare Reihen und Integrale" by M. Fujiwara, 323–329; "On the indeterminate form ∞/∞" by T. Hayashi, 330–336 (in Japanese).

Transactions of the Royal Society of Canada, volume 12, series III, Mathematical, physical and chemical sciences, December, 1918, and March, 1919: "Concerning the integrals of Leleuvre" by C. T. Sullivan, 171–184; "Rational plane unharmonic cubics" by A. M. Harding, 185–194.

AMERICAN DOCTORAL DISSERTATIONS.

R. W. Brink, "Some integral tests for the convergence and divergence of infinite series." *Published under the title:* "A new integral test for the convergence and divergence of infinite series," *Transactions of the American Mathematical Society*, 1918, volume 19, pp. 186–204. (Harvard, 1916.)

L. R. Ford, "On rational approximations to an irrational complex number," *Transactions of the American Mathematical Society*, 1918, volume 19, pp. 1–42. (Harvard, 1917.)

M. T. Hu, "Linear integro-differential equations with a boundary condition," *Transactions of the Amerìean Mathematical Society*, 1918, volume 19, pp. 363–407. (Harvard, 1917.)

W. E. Milne, "On the degree of convergence of Birkhoff's series." *Portions published as:* "On certain asymptotic expressions in the theory of linear differential equations," *Proceedings of the National Academy*, 1916, volume 2, pp. 543–545; "Note on asymptotic expressions in the theory of linear differential equations," *Bulletin of the American Mathematical Society*, 1917, volume 23, pp. 166–169. (Harvard, 1915.)

C. E. Wilder, "Problems in the theory of ordinary linear differential equations with auxiliary conditions at more than two points." *Portions published as:* "Expansion problems of ordinary linear differential equations with auxiliary conditions at more than two points," *Transactions of the American Mathematical Society*, 1917, volume 18, pp. 415–442. (Harvard, 1915.)

UNDERGRADUATE MATHEMATICS CLUBS.

Edited by U. G. Mitchell, University of Kansas, Lawrence.

CLUB ACTIVITIES.

The Mathematics Club of Albion College, Albion, Mich. [*1918*, 354–357.]

No meetings of this club were held during the period of the S. A. T. C. The first meeting of the year 1918–19 was held on January 21, 1919, and meetings were held regularly every other week thereafter, or as nearly according to this program as possible. Ten men and twelve women constituted the membership of the club for the year. Lieutenants W. Clarke Dean '21, and Murrey Fox '19, and Captain Jesse Campbell '19 returned to the club after having been in war service.

Officers for the year 1918–19 were: President, Carla Kennedy '20; vice-president, Esther Pearl '20; secretary-treasurer, Donald Alexander '20; program committee: the vice-president, the secretary-treasurer and Floyd Harper '20.

The usual program for each meeting is as follows: (1) roll-call, each member responding to his name by a very brief discussion of an assigned topic; (2) short talk of the evening, limited to ten minutes; (3) long talk, occupying 20 to 30 minutes; (4) general discussion of any of the topics of the evening; (5) critic's report (the critic is usually a student).

Programs for 1918–19 are indicated below [(1) roll-call, (2) short talk, (3) long talk]. The short talks for the year were biographical.

January 21, 1919: Organization and election of officers.

February 4: (1) "A mathematical current event;" (2) "Thales" by Thelma Sharp '21; (3) President's address, "Mathematics applied" by Carla Kennedy '20.

February 18: (1) "A mathematical symbol, its meaning and origin;" (2) "Pythagoras" by Gertrude Pratt '21; (3) "Development and use of determinants" by Floyd Harper '20.

March 11: (1) "Special curves, equation, history and use;" (2) "Life of Euclid" by Christine Niemann '21; (3) "My experiences as a teacher of high-school mathematics" by Margaret Courtright '19.

March 25: (1) "An original mathematical jingle." (2) "Archimedes" by Donald Herrick '21; (3) "Mathematics applied to war" by Lieutenant Clark Dean '21.

April 22: (1) "Some interesting application of mathematics:" (2) "Napier" by Edgar Smith '21; (3) "Mathematics and anti-mathematics" by Vera Junkin '19.

May 6: (1) "Some desirable characteristics that I observed in my high-school teacher of mathematics;" (2) "Descartes" by Esther Pearl '20; (3) "Indeterminate forms in trigonometry" by Esther Pearl '20.

May 20: (1) None; (2) None; (3) "The relation of the teacher to the community" by Elizabeth Gordon '21.
General discussion: "How can a teacher best enter into the community life" led by Miss Gordon.

June 3: Social evening and election of officers. The officers elected for 1919–20 are: President, Esther Pearl '20; vice-president, Joyce Hadaway '20; secretary-treasurer, Almyra K. Priest '20; member of program committee, Elizabeth Gordon '21.

TOPICS FOR CLUB PROGRAMS.

16. Codes and Ciphers.

The devising of codes and ciphers and of methods for solving them is closely allied to mathematics. In fact, since every system of secret writing must be based upon a certain fundamental set of symbols or sounds, all problems of deciphering such messages are essentially problems in permutations and combinations. The interest in the subject for students of mathematics is doubtless as much in the challenge to mathematical mastery as to the fascination of mystery.

The art of occult writing dates back to the ancient Greeks. The Spartans are credited with having sent messages by tattooing them upon the bodies of slaves. Sometimes, for greater secrecy, a slave whose scalp had been shaved and tattooed was not allowed to depart until his hair had grown long enough to conceal completely the message. When the slave had reached his destination the shaving of his scalp again revealed the message. The first record of secret writing on parchment, however, is probably that given by Plutarch in his life of Lysander where he gives[1] the following description of the manner of transmitting to that commander the order for his return:

> This scroll is made up thus: when the Ephors send an admiral or general on his way, they take two round pieces of wood, both exactly of a length and thickness, and cut even to one another; they keep one themselves and the other they give to the person they send forth; and these pieces of wood they call *scytales*. When, therefore, they have occasion to communicate any secret or important matter, making a scroll of parchment long and narrow like a leathern thong, they roll it about their own staff of wood, leaving no space void between, but covering the surface of the staff with the scroll all over. When they have done this, they take off the scroll, and send it to the general without the wood. He, when he has received it, can read nothing of the writing, because the words and letters are all broken up; but taking his own staff, he winds the slip of the scroll about it, so that this folding, restoring all the parts into the same order that they were in before, and putting what comes first into connection with what follows, brings the whole consecutive contents to view round the outside. And this scroll is called a *staff*, after the name of the wood, as a thing measured is by the name of the measure.

From Lysander's time (about 400 B.C.) to the present, great use has been made of secret writing by government officials in various connections of which the military has been the most important. A considerable number of special works on the subject have been written[2] but with the possible exception of Klüber's work, which seems to be the most widely known, these are not very likely to be available to most American students. The most available source for a brief discussion of the development of ciphers is likely to be the articles "Cryptography" by John Eglinton Bailey in recent editions of the *Encyclopædia*

---

[1] *Plutarch's Lives*, the translation called Dryden's, corrected from the Greek and revised by A. H. Clough, in 5 vols. (Boston, Little, Brown & Co., 1905), Vol. III, pp. 125–126. A parallel rendering of the same passage is found in John and William Langhorne's translation (New York, 1858), p. 314.

[2] Some of those most frequently cited are:

Trithemius, John, *Polygraphia*, cited as published in 1500 and in various later editions.

Portae, J. B., *De furtivis literarum notis*, Neapoli, 1563, and 1602, Londoni, 1591; another edition: *De occultis literarum notis*, Montisbeligardi, 1593, Argentorati (Strassburg), 1603 and 1606. Discusses different modes of secret writing, of which one hundred and eighty are explained, and a method proposed by which they can be multiplied ad infinitum.

Schott, Kasper, *De Magia Universali*, Würzburg, 1676.

Klüber, J. L., *Kryptographik*, Tübingen, 1809.

Fleissner, *Handbuch der Kryptographik*, Vienna, 1881.

Delastelle, F., *Cryptographie*, Paris, 1902.

Brittanica and similar articles in several other encyclopædias. A classification of ciphers and a considerable number of interesting examples are given by Ball in his *Mathematical Recreations and Essays*.[1] But the most interesting illustrations and historically important examples are contained in various articles[2] printed in periodical magazines to be found in nearly every university or large public library.

Ciphers and codes are both based upon substitutions, the distinction being in the unit chosen as the basis of the substitution. A cipher is based upon the substitution of symbols for letters and a code is based upon the substitution of words or symbols for words. For example the two lines

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
+	∧	%	*	=	/	$	÷	π	?	d	h	4	k	b	v	6	8	0	(	)	√	l	a	1	t

could be made the basis of a cipher by agreeing that each letter in the upper line should always be represented by the character immediately beneath it in the second line. In this simple cipher the message "The Americans are coming" would read "(÷= +4=8π%+k0 +8= %b4πk$". Such a cipher could be improved by the further agreement that any character not appearing in the second of the two lines forming its basis should be considered as a "dead" or "null" character. By the use of these "null" characters as space fillers the division into words, which is of great aid in deciphering, could be avoided. However, any considerable message written in so simple a cipher as the above would be read in a very few minutes by an expert, since the normal relative frequency of occurrence[3] of letters in English is:

---

[1] Fifth ed. (London, 1911), pp. 395–423; fourth ed. (1905), pp. 293–322.

[2] Of American articles appearing before the recent great war the following may be cited:

Century Magazine, Vol. 63, pp. 83–92, "Secret Writing, the Ciphers of the Ancients and some of those in Modern Use," by John H. Haswell.

Harper's Monthly, Vol. 97, pp. 105–109, "A Rebel Cipher Dispatch" by David Homer Bates. The author was manager and cipher-operator for the U. S. Military Telegraph Corps at Washington from 1861 to 1865. He describes ciphers used on both sides during the Civil War. Much other interesting information is given by the same author in an article entitled "Lincoln in the Telegraph Office," *Century Magazine*, Vol. 74, pp. 290–306.

North American Review, Vol. 128, 315–325, "Cryptography in Politics," by John R. G. Hassard. Gives examples of various ciphers and discusses some of the cipher telegrams connected with the presidential election of 1876. Other information concerning these cipher telegrams is given in the *Nation*, Vol. 27, p. 234, p. 250 and Vol. 28, p. 112.

Cosmopolitan, Vol. 36, pp. 475–478, 584–590, 715–718, three excellent articles on "Cryptography" by George Wilkes. Gives many examples of interesting and historical ciphers.

Bookman, Vol. 28, pp. 450–451, "Poe and Secret Writing," by Firman Dredd.

[3] The table given is from an article "Enciphering and Deciphering Codes" by Frank Morgan, of Fort Leavenworth, *Scientific American*, Vol. cxiii, No. 8 (August 21, 1915), p. 159. After giving an example of solving a much more difficult cipher message Mr. Morgan says: "We may say here that all practicable military ciphers are so marked by characteristic arrangement of the letters that no reasonably expert cipher man will be long in doubt as to the general method of enciphering. . . . A single short message would give trouble but military messages generally have fifty or more words."

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
20	4	8	11	33	6	5	16	17	1	2	10	8	19	21	6	$\frac{1}{4}$	18	17	23	8	3	5	1	5	1.

As an illustration of code,[1] suppose that a German spy and his correspondents agree upon the following substitutions:

a = the
French ship = market
sailed from New York = price
sailed from Boston = quotation
to-day = is
for Marseilles = any even number
for Bordeaux = any number with a fraction.

The intelligence that "A French ship sailed from New York to-day for Marseilles" in this code becomes the innocent business message "The market price is 110." By a slight change of wording, "The market quotation is $110\frac{1}{2}$" carries the information that "A French ship sailed from Boston to-day for Bordeaux."

Curiously enough, ciphers, which have been so widely used for secret writing and which were invented for that purpose, are not as securely secret as codes, which owe their development to their usefulness and economy in cabling commercial messages. Ciphers will, however, continue to be used where only *temporary* secrecy is desired, because, as Mr. Strother says, "cipher messages can be written and translated (by one's correspondent) without any equipment, like a code book, and much more rapidly than code. Thus, if a general in the field wishes to send a message ordering a colonel to advance in two hours, he sends it in cipher, because it would take the enemy more than two hours to decipher the message even if he intercepted it immediately, and because after the two hours have elapsed the information in the message would be of no value to him."

The recent great war not only led to renewed interest[2] in secret writing but also to the development of new forms. German spies made large use of geometric figures, drawings, sketches and pictures[3] as well as ciphers, codes and enciphered

---

[1] Cf. Strother, French, "German Codes and Ciphers," *World's Work*, June, 1918, p. 144.

[2] The following articles have appeared in the *Scientific American* during the war:

Brewton, William W., "The Science of the Cipher and an Explanation of Bacon's Undecipherable System," *Scientific American Supplement*, Vol. LXXIX, No. 2059 (June 19, 1915), pp. 394–395.

Edwards, E. C., "Cipher Codes and their Uses," *Sci. Am.*, Vol. CXIII, No. 1 (July 3 1915), p. 9.

Morgan, Frank, "Enciphering and Deciphering Codes," *Sci. Am.*, Vol. CXIII, No. 8 (August 21, 1915), p. 159.

Paddock, Ira J., "Cipher Codes Simplified," *Sci. Am.*, Vol. CXIII, No. 13 (Sept. 25, 1915), p. 271.

Woodworth, H. S., "A Simple Cipher Code," *Sci. Am.*, Vol. CXIII, No. 14 (Oct. 2, 1915), p. 291. Described a code adaptable to use with a slide rule.

Berkel, Ernest, "A Telegraphic Cryptogram," *Sci. Am.*, Vol. CXIII, No. 24 (Dec. 11, 1915), p. 519. Gives a convenient method for using figures in telegraphic messages.

[3] See in this connection the following:

Post, Melville Davisson, "German War Ciphers," *Everybody's Magazine*, June, 1918, pp. 28–34. Gives examples of diagrams and sketches. According to Mr. Post, the victory at the Marne was probably due, in part, to the amazing good fortune codes. In spite of the fact that the Allies controlled all overseas mails and cables, the German Government was apparently able to communicate at will, for a time at least, with its embassies and agents everywhere.

It would seem as if no article on this subject should omit a reference to the work of John Wallis, who has been called by D. E. Smith[1] "one of the world's greatest decipherers of cryptic writing," or to Francis Bacon's famous biliteral cipher[2] and Ignatius Donnelly's remarkable attempt[3] to prove, by means of a cipher, that Bacon was the author of Shakespeare's works.

Readers of Edgar Allan Poe's "Gold Bug" are probably aware of his belief that every cipher could be resolved and his challenge[4] to his readers to submit any which he could not decipher.

If any of our readers have never read Conan Doyle's "Adventures of the Dancing Man" a mention of it in this connection may lead to the enjoyment of its delightful mystery.

PROBLEMS AND SOLUTIONS.

EDITED BY B. F. FINKEL AND OTTO DUNKEL.

Send all communications about problems to B. F. FINKEL, Springfield, Mo.

PROBLEMS FOR SOLUTION.

2788. Proposed by WARREN WEAVER, University of Wisconsin.

Out of a freshman class of one thousand, various quiz sections are chosen by chance. After a semester's work A is found to stand 12th in a section of 18 students, and B is found to stand 18th

---

of the French war office in obtaining, by an extraordinary accident, which can not now be made public, the key to the German radiograph cipher code. "General Joffre knew the German orders wherever the radiograph signal was used in the advance on Paris. And it is possible that the knowledge of the radiograph code enabled the American Government to decipher the messages sent from the great wireless station at Nauen to Count von Luxburg, and so to make public the vast system of German intrigue that has amazed the world" (p. 29).

Strother, French, "Fighting Germany's Spies," *World's Work*, June, 1918, pp. 134–153. Gives descriptions and examples of the "Playfair" cipher (used by the British army in the field and pronounced by Mr. Strother "the cleverest transposition cipher ever devised"), the "Chess Board" cipher and the Bolo Pasha code.

Literary Digest, "A Graphic Spy Code," Vol. 56, p. 38, and "Keeping Government Cipher-Codes Secret," Vol. 51, pp. 546–548.

[1] Cf., Smith, D. E., "John Wallis as a Cryptographer" *Bulletin of the American Mathematical Society*, Vol. 24, No. 2 (Nov. 1917) pp. 82–96.

[2] *The Works of Francis Bacon, Baron of Verulam, Viscount of St. Alban, and Lord High Chancellor of England*, collected and edited by James Spedding, Robt. Leslie Ellis and Douglas Denon Heath (London, 1879), Vol. I, pp. 659–661. In a note on p. 843 Spedding credits the idea of a biliteral cipher, which Bacon seems to claim as his own, to John Baptist Porta (cf. *l.c.* above) although employed by him in a different manner.

[3] Donnelly, Ignatius, "The Great Cryptogram," R. S. Peale & Co., Chicago, N. Y., London, 1888.

[4] *The Works of Edgar Allan Poe*, with an introduction and a memoir by Richard Henry Stoddard (A. C. Armstrong & Son, N. Y., 1884), Vol. I, pp. 431–451. This essay on "Cryptography" contains, according to the editor, all that Poe had to say of importance on the subject. The challenge, which was first printed in *Graham's Magazine* for July, 1841, is reprinted on p. 442.

In Stedman and Woodberry's edition of Poe's works (Chicago, 1896) the essay on "Cryptography" appears in volume 9, pp. 260–278.